

1 **CLAIMS**

2

3 1. A method comprising:

4 receiving an event, the event comprising a data section containing a set of
5 strings each containing an event field;

6 referencing a definition table to determine locations of event fields in the
7 data section of the event; and

8 storing the event fields in a database record corresponding to event field
9 locations referenced from the definition table.

10

11 2. The method as recited in Claim 1, wherein the event fields are in the form
12 of a data value.

13

14 3. The method as recited in Claim 1, further comprising generating the
15 definition table by:

16 selecting one or more specific types of event fields from a event schema;
17 ascertaining locations of the specific types of event fields in the event
18 schema; and

19 storing the locations of the specific types of event fields in the definition
20 table.

21

22 4. The method as recited in Claim 1, wherein a portion of the set of strings
23 pertains to a security sensitive transaction.

1 5. The method as recited in Claim 1, wherein the event is received from an
2 event log.

3
4 6. The method as recited in Claim 1, wherein the event further comprises an
5 event header section that includes an event identification indicating a select one of
6 a plurality of different types of events.

7
8 7. One or more computer-readable media comprising computer-executable
9 instructions that, when executed, perform the method as recited in claim 1.

10
11 8. A method comprising:

12 receiving an event that contains, respectively, an event identification
13 indicating a select one of a plurality of different types of events and one or more
14 sets of strings with each string containing an event field;

15 identifying the event indication in the event;

16 locating an entry in a definition table corresponding to the event
17 identification of the received event;

18 from the located entry of the event in the definition table, the located entry
19 containing locations of types of event fields for the event, using the definition
20 table as a reference to locate event fields in the received event; and

21 for the received event, storing the located event fields in records of an event
22 database corresponding to the types of event fields.

23
24 9. The method as recited in Claim 8, wherein the values in the event fields are
25 in the form of a data value.

1
2 10. The method as recited in Claim 8, further comprising:
3 generating the definition table by:
4 selecting one or more specific types of event fields from a event schema;
5 ascertaining locations of the specific types of event fields in the event
6 schema; and
7 storing the locations of the specific types of event fields in the definition
8 table.
9
10

11 11. The method as recited in Claim 8, wherein a portion of the set of strings
12 pertains to a security sensitive transaction.
13
14

15 12. The method as recited in Claim 8, wherein the event is received from a
16 security log.
17
18

19 13. One or more computer-readable media comprising computer-executable
20 instructions that, when executed, perform the method as recited in claim 8.
21
22

23 14. A system for maintaining records of events comprising:
24 an event receiver module, configured to receive an event that contains,
25 respectively, an event identification indicator and strings containing event fields
each specifying a different component aspects of the event; and
 an event-processing module, configured to reference an event definition
table to determine locations of event fields in the event, and store the event fields
26
27

1 in a record of a database according to the different component aspect specified by
2 the event field.

3

4 15. The system as recited in Claim 14, further comprising a computer that
5 maintains the event receiver module and the event-processing module.

6

7 16. The system as recited in Claim 14, further comprising a client computer
8 that performs certain actions that are recorded as an event.

9

10 17. The system as recited in Claim 14, wherein one or more the event pertains
11 to a security sensitive transaction.

12

13 18. The system as recited in Claim 14, wherein one or more of the event fields
14 pertain to a client logging-on to a network.

15

16 19. The system as recited in Claim 14, wherein one or more of the event fields
17 pertain to a client opening a file.

18

19 20. The system as recited in Claim 14, wherein one or more of the event fields
20 pertain to a client performing certain application level tasks.

21

22 21. The system as recited in Claim 14, wherein one or more of the event fields
23 pertain to a client administering passwords.

1 22. The system as recited in Claim 14, wherein one or more of the event fields
2 pertain to a client changing passwords.

3

4 23. The system as recited in Claim 14, wherein one or more of the event fields
5 pertain to a client accessing a particular object.

6

7 24. The system as recited in Claim 14, further comprising a definition-module,
8 configured to generate a definition table by:

9 selecting one or more specific types of event fields from a event schema;

10 ascertaining locations of the specific types of event fields in the event
11 schema; and

12 storing the locations of the specific types of event fields in the definition
13 table.

14

15 25. One or more computer-readable media having stored thereon a computer
16 program that, when executed by one or more processors, causes the one or more
17 processors to:

18 receive an event that contains, respectively, an event identification
19 indicating a select one of a plurality of different types of events and one or more
20 sets of strings with each string containing an event field;

21 identify the event indication in the event;

22 locate an entry in a definition table corresponding to the event identification
23 of the received event;

1 from the located entry of the event in the definition table, the located entry
2 containing locations of types of event fields for the event, use the definition table
3 as a reference to locate event fields in the received event; and

4 for the received event, store the located event fields in records of an event
5 database corresponding to the types of event fields..

6

7 26. One or more computer-readable media as recited in Claim 25, that when
8 executed by one or more processors, further causes the one or more processors to:

9 generate the event definition table by:

10 selecting one or more specific types of event fields from a event schema;

11 ascertaining locations of the specific types of event fields in the event
12 schema; and

13 storing the locations of the specific types of event fields in the definition
14 table.

15

16 27. A system for storing events, comprising:

17 client computers, configured to generate events that contain, respectively,
18 an event identification indicator and one or more strings, the strings containing
19 event fields;

20 an event definition table specifying locations of the event fields; and

21 means for storing the one or more event fields from generated events in
22 records of a database appurtenant to the locations specified by the event definition
23 table.

1 28. The system as recited in Claim 27, further comprising a means for
2 generating the event definition table comprising:

3 means for selecting one or more specific types of event fields from a event
4 schema;

5 means for ascertaining locations of the specific types of event fields in the
6 event schema; and

7 means for storing the locations of the specific types of event fields in the
8 definition table..

9
10 29. The system as recited in Claim 27, wherein the means for storing the one or
11 more event fields in the database record is performed by an event-processing
12 module of a computer.

13
14 30. The system as recited in Claim 27, wherein the event identification
15 indicator identifies a type of security sensitive event performed by the computer.

16
17 31. One or more computer-readable media comprising computer executable
18 instructions that, when executed, direct a computer to:

19 generate events that contain, respectively, an event identification and one or
20 more event descriptions, the event descriptions containing one or more values in
21 the event fields, and store the events strings in a log when a security sensitive
22 event is performed; and

23 store the events in a database in a manner to enable values in the event
24 fields to be independently searched through the use of an event definition table
25 containing mappings of the event descriptions for each event identification, the

1 mappings including the locations of one or more values in the event fields
2 contained within the event descriptions.

3
4 32. One or more computer-readable media as recited in Claim 31, further
5 comprising computer executable instructions that, when executed, direct the
6 computer to parse the event descriptions to identify one or more values in the
7 event fields.

8
9 33. One or more computer-readable media as recited in Claim 31, further
10 comprising computer executable instructions that, when executed, direct the
11 computer to generate the event definition table by:

12 selecting one or more value types from the event;
13 ascertaining locations of the values in the event fields in the event that
14 correspond to the one or more selected value types; and
15 storing the location of the values in the event fields in fields of the
16 definition table that corresponding to the one or more selected value types.